IN THE CLAIMS

A complete list of claims is presented below with amendments marked up:

1.   (Currently amended) A method, comprising:

receiving a plurality of reports from a community of users, each report identifying

an email message as spam or not spam, wherein each report comprises at least one

signature based on a content of the email message; and

determining if the email message is spam based on a number of the reports

received from the community of users, and a trust factor associated with each user.

2.   (Original) The method of claim 1, further comprising maintaining a

database of email messages determined as being spam.

3.   (Original) The method of claim 2, further comprising providing

notifications to the community of users of email messages stored in the database and

determined as being spam.

4.   (Original) The method of claim 3, wherein each notification is in response

to a request received from a user in the community for an indication on whether an

identified message is spam.

5.   (Canceled).

6.   (Original) The method of claim 1, wherein the trust factor is based on an

indication of how accurately previous reports sent by the user identified email messages

as spam.

7.   (Currently amended) A server, comprising:

a processor; and

a memory coupled to the processor, the memory storing instructions which when

executed by the processor cause the processor to perform a method, comprising:

        receiving a plurality of reports from a community of users, each report

identifying an email message as spam or not spam, wherein each report comprises at least

one signature based on a content of the email message; and

        determining if the email message is spam based on a number of the reports

received from the community of users, and a trust factor associated with each user.

8.   (Original) The server of claim 7, wherein the method further comprises

maintaining a database of email messages determined as being spam.

9.   (Original) The server of claim 8, wherein the method further comprises

providing notifications to the community of users of email messages stored in the

database and determined as being spam.

10.   (Original) The server of claim 9, wherein each notification is in response

to a request received from a user in the community for an indication on whether an

identified message is spam.

11.   (Canceled).

12.   (Original) The server of claim 7, wherein the trust factor is based on an indication of how accurately previous reports sent by the sender identified email messages as spam.

13.   (Currently amended) A ~~computer-readable~~ recordable-type medium having stored thereon a sequence of instructions which when executed by a computer, cause the computer to perform a method comprising:

receiving a plurality of reports from a community of users, each report identifying an email message as spam or not spam, wherein each report comprises at least one signature based on a content of the email message; and

determining if the email message is spam based on a number of the reports received from the community of users, and a trust factor associated with each user.

14.   (Currently amended) The ~~computer-readable~~ recordable-type medium of claim 13, wherein the method further comprises maintaining a database of email messages determined as being spam.

15.   (Currently amended) The ~~computer-readable~~ recordable-type medium of claim 14, wherein the method further comprises providing notifications to the community of users of email messages stored in the database and determined as being spam.

16.   (Currently amended) The ~~computer-readable~~ recordable-type medium of claim 15, wherein each notification is in response to a request received from a user in the community for an indication on whether an identified message is spam.

17.   (Canceled).

18.   (Currently amended) The ~~computer-readable~~ recordable-type medium of claim 14, wherein the trust factor is based on an indication of how accurately previous reports sent by the sender identified email messages as spam.

19.   (New) The method of claim 1, wherein the at least one signature comprises a hash calculated based on the content of the email message.

20.   (New) The method of claim 2, further comprising:

using the at least one signature as a key to store the email message in the database if the email message is determined to be spam.

21.   (New) The server of claim 7, wherein the at least one signature comprises a hash calculated based on the content of the email message.

22.   (New) The server of claim 2, wherein the method further comprises:

using the at least one signature as a key to store the email message in the database if the email message is determined to be spam.

23.   (New) The recordable-type medium of claim 13, wherein the at least one

signature comprises a hash calculated based on the content of the email message.

24.   (New) The recordable-type medium of claim 14, wherein the method

further comprises:

using the at least one signature as a key to store the email message in the database

if the email message is determined to be spam.